CLAIMS

What is claimed is:

1. A method for enabling a firewall to securely pass encrypted data, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a fist security policy;

exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

requesting, based at least in part upon the second security policy, the first encryption key; wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

passing encrypted data when it is determined that the first encryption key is received.

2. The method of claim 1, further comprising:

not allowing encrypted data to pass when it is determined that the first encryption key is not received.

3. The method of claim 1, wherein the step of detecting an exchange of a first encryption key further comprises:

monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

4. A method for enabling a firewall to selectively monitor encrypted data traffic, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data

exchanged between the firewall and the host device according to a second security policy;

requesting, based at least in part upon the second security policy, the first encryption key wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

decrypting encrypted data, using the first encryption key, according to a predetermined monitoring policy.

5. A method for enabling a firewall to selectively pass protocols and services, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and

the host device according to a second security policy;

requesting, based at least in part upon the second security policy, the first encryption key, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy;

decrypting encrypted data, using the first encryption key; and

applying a predetermined filtering policy to the decrypted data.

6. The method of claim 5, further comprising:

re-encrypting the decrypted data.

7. A firewall apparatus that securely passes encrypted data, the apparatus comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the

first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

a key requestor for requesting, based at least in part upon the second security policy, the first encryption key; wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

an encrypted data passer for passing encrypted data when it is determined that the first encryption key is received.

8. The apparatus of claim 7, further comprising:

an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received.

9. The apparatus of claim 7, wherein the exchange detector further comprises:

a monitor for monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

10. A firewall apparatus for selectively monitoring encrypted data traffic, the apparatus comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

a requestor for requesting, based at least in part upon the second security policy, the first encryption key wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

a decryptor for decrypting encrypted data, using the first encryption key, according to a predetermined monitoring policy.

11. A firewall apparatus for selectively passing protocols and services, the method comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

a requestor for requesting, based at least in part upon the second security policy, the first encryption key, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy;

a decryptor for decrypting encrypted data, using the first encryption key; and

a filter for applying a predetermined filtering policy to the decrypted data.

12. The apparatus of claim 11, further comprising:

an encryptor for re-encrypting the decrypted data.